CSO
SECURITY AND RISK

🖶 Print ☒ Close Window

From: www.csoonline.com

Five cloud security trends experts see for 2011

What do IT security practitioners expect to be major cloud security issues in 2011? Here are five things to watch for.

by Bob Violino, CSO

December 16, 2010

What do CSOs and other IT security experts expect to be top-of-mind cloud security issues in 2011? Here are five things to watch for in the coming year:

1. Smart phone data slinging . More users will be accessing large amounts of data on the devices of their choice, says Randy Barr, CSO at Qualys Inc. and member of the Cloud Security Alliance (CSA). "This comes with a lot of unaddressed security issues," Barr says. "We can expect new solutions to address mobile devices, but could see a large data breach to expose the issue of mobile security before we see a solution." Among the possible scenarios, Barr says, are insecure cloud-based backup and highly confidential data on mobile devices."There are some interesting inter-dependencies when using multiple cloud services on mobile devices, with possibly different security models and assumptions," he says. A hacked cloud provider could provide mass access to confidential mobile device data when mobile users are using cloud-based mobile device support, he says. In addition, loss or theft of mobile device could provide root-level access to cloud services and data. Mobile apps are often providing direct and automated access to cloud services and data, he says. If an admin-level person's mobile device is stolen, this could be a major threat to highly confidential data or even cloud services administered by such a person from an insecure mobile device.

MORE ABOUT CLOUD SECURITY

- 2010: Security for large-company cloud providers
- 2010: In security outsourcers we trust
- 2010: Akamai releases 'game changing' cloud-based payment service
- 2008: Cloud security strategies: Where does IDS fit in?

2. Need for better access control and identity management."The cloud by nature is highly virtualized and highly federated, and you need an approach to establish control and manage identities across your cloud and other peoples' clouds," says Alan Boehme, senior vice president of IT strategy and architecture at financial services firm ING. "There are some third parties that have delivered products and services that will address these issues, but they might not be adequate for large enterprises that have a mix of legacy and cloud components."

3. Ongoing compliance concerns."I think that compliance, especially PCI, is likely to continue to be a security issue," says Andy Ellis, CSO at Akamai. "Organizations still often need to come to grips with completely different processes that they have for managing data and apps in the cloud. And I think we will hear more rumblings about healthcare data in the cloud."

4. Risk of multiple cloud tenants. Given that most cloud services make heavy use of virtualization technology, the risks associated with multiple organizations' data housed on a single physical hypervisor platform exist, and will continue to unless specific segmentation measures are enacted, says Dave Shackleford, director of security assessments and risk & compliance at Sword & Shield Enterprise Security, and a member of the faculty of research firm IANS. Although it is assumed that virtual machines and virtual network components are 'separated by default', flaws and potential weaknesses in hypervisor platforms have been documented that could cause segmentation issues.

The most well-documented flaw was the one noted last year by Kostya Korchinsky of Immunity, where he "broke out" of a VMware Virtual Machine and executed a program on the underlying hypervisor system with a proof-of-concept tool called CloudBurst, Shackleford says. And in 2008 Core Security found a directory flaw that could allow an attacker to access files on the hypervisor from the virtual machine, he says.

5. Emergence of cloud standards and certifications. Because security will be evaluated when choosing cloud services, standards and certifications will be extremely important to help customers gauge how secure their data will be kept, Barr says. Cloud users will continue to leverage their existing processes for evaluating the security postures of cloud providers, but will begin looking at some of the more popular organizations developing guidance and standards, he says.

Share your insight on the current state of information security practices and challenges.
PARTICIPATE IN THE 9TH GLOBAL INFORMATION SECURITY SURVEY.
CIO
CS